

# MATEMATICA DISCRETA

(9 CFU)

prof. **Fabio GAVARINI**

(codocente prof.ssa **Ilaria DAMIANI**)

-----

## INSIEMI, CORRISPONDENZE, RELAZIONI

Insiemi; sottoinsiemi, sovrainsiemi, inclusione. L'insieme delle parti di un insieme. Famiglie. Operazioni tra insiemi e loro proprietà notevoli; insiemi disgiunti. Partizioni di un insieme.

Corrispondenze tra insiemi. Immagine o controimmagine di sottoinsiemi; corrispondenza inversa; operazioni tra corrispondenze, e loro proprietà notevoli; corrispondenza complementare, corrispondenza inversa.

Funzioni. Caratterizzazione delle famiglie come funzioni. Restrizione di una funzione. Funzioni iniettive, suriettive o biiettive; biiettività e corrispondenza inversa. Composizione di funzioni; funzioni invertibili e loro caratterizzazioni.

Funzioni caratteristiche in un insieme. Biiezione naturale tra insieme delle parti insieme delle funzioni caratteristiche.

Relazioni in un insieme. Proprietà notevoli per una relazione. Relazioni di preordine, relazioni d'ordine, relazioni di equivalenza. La congruenza modulo  $n$  tra interi. L'equivalenza associata a una funzione. Classi di equivalenza, rappresentanti; insieme quoziente. Biiezione tra equivalenze in  $X$  e partizioni di  $X$ . Decomposizione canonica di una funzione.

Operazioni (binarie) in un insieme, e loro proprietà notevoli.

**Bibliografia:** [Ca] [Capitolo I, paragrafi 1, 2, 3 e 4](#) - [G-P] files [Insiemi](#), [Funzioni e cardinalità](#), [Relazioni 1](#), [Gruppi, anelli, campi](#) - [L-L] Chapters 1, 2 e 3; Appendix B - [PC] Capitolo 1, paragrafi 1, 2 e 3; Capitolo 4, paragrafo 1; Capitolo 5, paragrafi 1 e 2

**Videolezioni:** [Insiemi](#), [Corrispondenze](#), [Funzioni 1](#), [Funzioni 2](#), [Funzioni caratteristiche](#), [Relazioni](#), [Equivalenze 1](#), [Equivalenze 2](#), [Operazioni 1](#), [Operazioni 2](#)

## NUMERI NATURALI, CALCOLO COMBINATORIO

Il Sistema dei Numeri Naturali (=S.N.N.). Il Principio di Induzione Debole (=Pr.I.D.). Ordinamento, somma e prodotto tra naturali; i numeri formano un semianello in cui l'ordine è compatibile con le operazioni. Principio di Induzione Forte (=Pr.I.F.), Principio del Minimo (=Pr.M.): equivalenza tra Pr.I.D., Pr.I.F. e Pr. M. Dimostrazioni per induzione.

Divisione con resto tra naturali. Numerazione in base arbitraria: scrittura posizionale (di un naturale) in base arbitraria.

Calcolo del numero di: (1) funzioni da un insieme finito ad un altro ("disposizioni con ripetizione"); (2) funzioni *iniettive* da un insieme finito ad un altro ("disposizioni senza ripetizione"); (3) biiezioni tra due insiemi finiti (o permutazioni di un insieme finito in sé stesso) con  $n$  elementi: il *fattoriale* di  $n$ ; (4) sottoinsiemi con  $k$  elementi in un insieme con  $n$  elementi ("combinazioni di  $k$  elementi scelti tra  $n$ "): *coefficienti binomiali*. La formula di Newton per lo sviluppo delle potenze di un binomio e per lo sviluppo delle potenze di un multinomio. Proprietà notevoli dei coefficienti binomiali, e casi speciali. Il triangolo di Pascal-Tartaglia.

**Bibliografia:** [AaVv] file [Numeri naturali \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafi 1 e 5](#); [Capitolo II, paragrafo 2](#) - [G-P] files [Induzione](#), [Aritmetica sugli interi, etc. \(complementi\)](#), paragrafo 1 - [L-L] Chapter 1, section 8; Chapter 5, sections 1 to 5; Chapter 6, sections 1 to 3; Chapter 11, sections 3 - [PC] Capitolo 1, paragrafi 4 e 6; Capitolo 2, paragrafo 10

**Videolezioni:** [Naturali](#), [Induzione](#), [Divisione](#), [Numerazione](#)

# CARDINALITÀ, NUMERI CARDINALI

L'equipotenza tra insiemi. Cardinalità di un insieme, numeri cardinali. Insiemi finiti, o infiniti numerabili, o infiniti non numerabili. Ordinamento tra numeri cardinali; Teorema di Schroeder-Bernstein (*cenni di dimostrazione*).

Caratterizzazione degli insiemi numerabili. Il numerabile è il più piccolo dei cardinali infiniti. Equivalenza delle proprietà: (1)  $X$  è infinito, (2)  $c$ 'è una funzione iniettiva da  $\mathbf{N}$  ad  $X$ , (3)  $c$ 'è un sottoinsieme proprio di  $X$  equipotente a  $X$ .

1° Teorema di Cantor: L'unione di una famiglia finita (non vuota) o numerabile di insiemi numerabili è numerabile.

Esempi di applicazione del 1° Teorema di Cantor: gli insiemi  $\mathbf{Z}$ ,  $\mathbf{N} \times \mathbf{N}$  e  $\mathbf{Q}$  sono numerabili.

2° Teorema di Cantor: La cardinalità dell'insieme delle parti di  $X$  è strettamente maggiore della cardinalità di  $X$ .

I cardinali infiniti superiori  $\aleph_n$ . La cardinalità del continuo:  $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})|$ ; l'ipotesi del continuo generalizzata (*cenni*).

**Bibliografia**: [AaVv] file [Cardinalità \(D'Andrea\)](#) - [Ca] [Capitolo I, paragrafo 6](#) - [G-P] file [Funzioni e cardinalità](#), paragrafo 5 - [L-L] Chapter 3, section 7 - [PC] Capitolo 1, paragrafo 5

**Videolezioni**: [Cardinalità 1](#), [Cardinalità 2](#)

# NUMERI INTERI, CONGRUENZE, ARITMETICA MODULARE

Richiami sui numeri interi: operazioni, ordine, valore assoluto. Costruzione degli interi a partire dai naturali, come "naturali + i negativi". Anelli, domini, campi. Divisibilità; elementi invertibili, elementi associati. Elementi riducibili, elementi irriducibili, elementi primi; ogni primo è irriducibile. Fattorizzazioni banali, fattorizzazioni equivalenti.

Massimo comun divisore (=MCD) e minimo comun multiplo (=mcm). Elementi coprimi (=primi tra loro).

Divisione con resto tra interi: esistenza e unicità di quoziente e resto (positivo). Esistenza del MCD in  $\mathbf{Z}$ , e identità di Bézout per esso: calcolo con l'algoritmo euclideo delle divisioni successive. Tra i numeri interi, ogni irriducibile è primo.

Teorema Fondamentale dell'Aritmetica: esistenza e unicità di una fattorizzazione in irriducibili per interi non nulli e non invertibili. Teorema di Euclide: Esistono infiniti interi irriducibili (a due a due non associati).

Forma esplicita di  $MCD(a,b)$  e di  $mcm(a,b)$ ; la relazione  $MCD(a,b) mcm(a,b) = a b$ .

Equazioni diofantee: definizione, semplificazioni, criterio di risolubilità, algoritmo per il calcolo di una soluzione.

Congruenze in  $\mathbf{Z}$  (modulo  $n$ ). Ogni congruenza è una equivalenza; descrizione delle classi di congruenza e dell'insieme quoziente  $\mathbf{Z}_n$ . Somma e prodotto in  $\mathbf{Z}_n$ . Teorema:  $\mathbf{Z}_n$  è un anello commutativo unitario (*cenni di dimostrazione*). Criteri di divisibilità in  $\mathbf{Z}$ . Proposizione:  $\mathbf{Z}_n$  è un dominio  $\Leftrightarrow n$  è irriducibile (=primo)  $\Leftrightarrow \mathbf{Z}_n$  è un campo.

Equazioni congruenziali (in  $\mathbf{Z}$ ), equazioni modulari (in  $\mathbf{Z}_n$ ): semplificazioni, criterio di risolubilità, algoritmo risolutivo, insieme delle soluzioni. Il gruppo moltiplicativo  $U(\mathbf{Z}_n)$  degli elementi invertibili nell'anello  $\mathbf{Z}_n$ : criterio di invertibilità, calcolo dell'inverso; la funzione di Eulero.

Potenze in  $\mathbf{Z}_n$ : il Piccolo Teorema di Fermat, il Teorema di Eulero (*senza dimostrazione*); calcolo di potenze in  $\mathbf{Z}_n$ .

Sistemi di equazioni congruenziali. Sistemi in forma cinese; il Teorema Cinese del Resto (*senza dimostrazione*).

**Bibliografia**: [AaVv] files [Numeri interi \(D'Andrea\)](#), paragrafo 4, [Congruenze, aritmetica modulare\(D'Andrea\)](#), paragrafi 1 e 2 - [Ca] [Capitolo II, paragrafi da 1 a 6](#) - [G-P] files [Aritmetica sugli interi, congruenze, Teorema Cinese del Resto](#), [Aritmetica sugli interi, etc. \(complementi\)](#) - [L-L] Chapter 11, sections 1 to 9 - [PC] Capitolo 2, paragrafi da 1, 2, 3, 6, 7, 8 e 9

# INSIEMI ORDINATI, RETICOLI, ALGEBRE DI BOOLE, FUNZIONI BOOLEANE

Relazioni d'ordine; ordini totali, ordini buoni. Relazione di copertura, diagramma di Hasse. Sottoinsiemi ordinati, intervalli. Principio di Dualità per insiemi ordinati. Ordine prodotto e ordine lessicografico. Elementi minimali/massimali, minoranti/maggioranti, minimo/massimo, estremo inferiore/superiore per un sottoinsieme in un insieme ordinato  $E$ .

Reticoli (con duplice definizione). Principio di Dualità per reticoli. Limiti, complementi, distributività. Elementi  $v$ -riducibili o  $v$ -irriducibili; atomi. Teorema di  $v$ -Fattorizzazione (in  $v$ -irriducibili) per reticoli finiti. Teorema di  $v$ -Fattorizzazione Unica (in  $v$ -irriducibili) per reticoli finiti distributivi. Teorema di  $v$ -Fattorizzazione  $U$ -nica (in atomi) per reticoli finiti distributivi complementati (=algebre di Boole). Isomorfismi tra reticoli, reticoli isomorfi; sottoreticoli di un reticolo. Teorema: Un reticolo è distributivo  $\Leftrightarrow$  non ha sottoreticoli isomorfi a  $\mathbf{N}_5$  o a  $\mathbf{M}_5$  (*senza dimostrazione*).

Algebre di Boole (con duplice definizione). Principio di Dualità per algebre di Boole. Anelli booleani. Teorema di Equivalenza: "Algebra di Boole" e "anello booleano unitario" sono nozioni equivalenti (*soltanto la definizione delle corrispondenze*). Isomorfismi tra algebre di Boole, algebre di Boole isomorfe. Esempio: la biiezione canonica tra l'insieme delle parti  $\mathcal{P}(X)$  e l'insieme delle funzioni caratteristiche  $2^X$  è un isomorfismo di algebre di Boole. Teorema di Stone (finito): Ogni algebra di Boole finita è isomorfa all'insieme delle parti dell'insieme dei suoi atomi. Controesempio al Teorema di Stone (finito). Sottoalgebre di Boole. Teorema di Stone (generale): Ogni algebra di Boole è isomorfa a una sottoalgebra di Boole dell'insieme delle parti di un opportuno insieme (*senza dimostrazione*).

Funzioni booleane, polinomi booleani. Equivalenza tra polinomi booleani. Prodotti, prodotti fondamentali; somme di prodotti. Forma normale disgiuntiva di un polinomio; calcolo tramite (1) manipolazioni successive, o (2) "tavole di verità". Forme minimali di un polinomio booleano. Gli implicanti primi di un polinomio booleano. Somme di prodotti non ridondanti. Il *Metodo del Consenso* per calcolare la somma degli implicanti primi di  $f$ , e una sua forma minimale.

**Bibliografia:** [Ca] [Capitolo I, paragrafo 3\(B\)](#) - [G-P] files [Relazioni - 2](#) , [Reticoli](#) , [Algebre di Boole](#) , [Funzioni booleane](#) , [Forme minimali di una funzione polinomiale](#) - [L-L] Chapter 14, sections 1 to 5 and 7 to 11; Chapter 15, sections 1 to 9

**Videolezioni:** [Insiemi ordinati](#) , [Reticoli 1](#) , [Reticoli 2](#) , [Reticoli 3](#) , [Algebre di Boole 1](#) , [Algebre di Boole 2](#)

## (MULTI)GRAFI, (MULTI)DIGRAFI

Multidigrafi, multigrafi; il multigrafo soggiacente a un multidigrafo; sottomultidigrafi e sottomultigrafi. Unione (o "somma") di multidigrafi, o di multigrafi. Grado entrante, grado uscente, grado (totale) di un vertice in un multidigrafo; pozzi e sorgenti. Grado di un vertice in un multigrafo; vertici isolati, vertici pendenti (o "foglie"). Multidigrafi bipartiti, multigrafi bipartiti, digrafi bipartiti, digrafi funzionali. Grafi semplici, grafi regolari, grafi completi.

*Teorema ("Lemma delle Strette di Mano"):* (1) In ogni multigrafo finito, la somma dei gradi di tutti i vertici è uguale al doppio del numero degli spigoli del multigrafo. (2) In ogni multidigrafo finito, la somma dei gradi entranti di tutti i vertici e la somma dei gradi uscenti di tutti i vertici sono entrambe uguali al numero degli archi del multidigrafo.

Cammini, circuiti in multigrafi e in multidigrafi; connessione. Componenti connesse, ponti in un multigrafo.

*Proposizione:* Ogni multigrafo è l'unione delle sue componenti connesse.

La matrice di adiacenza di un multigrafo e di un multidigrafo. Calcolo del numero di cammini in un multi(di)grafo da un vertice a un altro tramite le potenze – per il prodotto righe per colonne - della matrice di adiacenza (o sua variante).

Cammini euleriani in un multi(di)grafo; multi(di)grafi euleriani o semieuleriani. *Teorema* di caratterizzazione dei multigrafi e multidigrafi euleriani o semieuleriani. L'*Algoritmo di Fleury* e l'*Algoritmo di Hierholzer* per il calcolo di un cammino euleriano (se esiste) in un multidigrafo o un multigrafo (*cenni*).

Alberi (non orientati), foreste; ogni foresta è unione di alberi (le sue componenti connesse).

*Teorema (caratterizzazione degli alberi):* Per ogni multigrafo  $G$ , le seguenti quattro proprietà sono equivalenti:

(a)  $G$  è un albero; (b)  $G$  è aciclico, ma se si aggiunge un qualsiasi nuovo spigolo si ottiene un grafo ciclico; (c) per ogni scelta di vertici  $u$  e  $v$  in  $G$  esiste uno ed un solo percorso da  $u$  a  $v$  in  $G$ ; (d)  $G$  è connesso, ma se si toglie un qualsiasi spigolo si ottiene un sottografo sconnesso (in altre parole, ogni spigolo in  $G$  è un ponte).

*Teorema (caratterizzazione degli alberi finiti):* Per ogni multigrafo  $G:=(V,E)$  con numero finito di vertici, le seguenti proprietà sono equivalenti: (a)  $G$  è un albero; (b)  $G$  è aciclico e  $|E|=|V|-1$ ; (c)  $G$  è connesso e  $|E|=|V|-1$ .

*Proposizione:* Ogni albero finito con almeno due vertici ha almeno due foglie.

Colorazioni di un multigrafo (*cenni*). Ogni albero è bipartito (in altre parole, è colorabile con due colori). Un multigrafo è bipartito se e soltanto se non possiede cicli (o circuiti) di lunghezza dispari (*esercizio*).

*Alberi ricoprenti* di un multigrafo; algoritmi di Kruskal per la costruzione di alberi ricoprenti.

**Bibliografia:** [L-L] Chapter 8, sections 1, 2, 3, 4, 5, 7, 8 and 11; Chapter 9, sections 1, 2, 3 and 5 - [Qua] [Breve Introduzione alla Teoria dei Grafi](#), Capitoli 1, 2, 4 e 6

• • • ☼ ☼ ☼ • • •

## TESTI (libri, dispense, videolezioni, ecc.) consigliati:

[AaVv] - Autori Varî, [Materiale vario disponibile in rete](#) (per gentile concessione degli autori)

[Ca] - G. Campanella, [Appunti di Algebra 1](#) (per gentile concessione dell'autore)

[Ga] - F. Gavarini, [Videolezioni varie](#)

[G-P] - L. Geatti, G. Pareschi, [Appunti vari](#) (per gentile concessione degli autori)

[L-L] - S. Lipschutz, M. Lipson, *Discrete Mathematics*, 3rd Edition, Schaum's Outlines, McGraw-Hill, 2007

[PC] - G. M. Piacentini Cattaneo, *Algebra - un approccio algoritmico*, ed. Decibel/Zanichelli, Padova, 1996

[Qua] - G. Quattrocchi, [Breve Introduzione alla Teoria dei Grafi](#) (per gentile concessione dell'autore)